CLAIMS:

1. A method comprising:

storing authorization data that defines an access control attribute and an associated regular expression specifying a textual pattern;

evaluating a command using the regular expression to determine whether the command matches the textual pattern; and

controlling access to configuration data of a device based on the evaluation.

2. The method of claim 1, wherein controlling access comprises allowing access to the configuration data when the textual pattern of the regular expression matches the command.

3. The method of claim 1, wherein controlling access comprises denying access to the configuration data when the textual pattern of the regular expression matches the command.

4. The method of claim 1, wherein storing authorization data comprises storing the authorization data as an authorization class that conforms to a class syntax.

5. The method of claim 1, wherein storing authorization data comprises storing authorization data that includes a course-grain access control attribute defining access control rights for respective groups of resources provided by the device, and controlling access comprises controlling access to the configuration data based on the course-grain access control attribute and the evaluation of the regular expression.

6. The method of claim 5, wherein the course-grain access control attribute comprises a set of permission bits, and each of the permission bits is associated with a respective group of the resources.

7. The method of claim 1, further comprising receiving the command from a client via a command line interface.

8. The method of claim 7, wherein evaluating the command comprises evaluating the command in real-time while the client inputs the command via the command line interface.

9. The method of claim 1, wherein the configuration data is arranged in the form of a multi-level configuration hierarchy having a plurality of objects, and each of the objects represents a portion of the configuration data that relates to one or more resources of the device.

10. The method of claim 9, wherein the objects have respective textual labels and the regular expression defines the textual pattern to match the textual labels of a set of one or more of the objects within the configuration hierarchy.

11. The method of claim 10, wherein evaluating the command comprises applying the regular expression to the command to determine whether the command specifies any of the objects within the set.

12. The method of claim 9, further comprising pre-processing the regular expression to automatically insert one or more meta-characters into the regular expression based on the hierarchical arrangement of the configuration data.

13. The method of claim 9, further comprising:

receiving the command from a client via a command line interface; and

pre-processing the regular expression so that the command is evaluated with the regular expression in real-time as the client enters the command.

14. The method of claim 13, wherein evaluating the command comprises evaluating the command with the pre-processed regular expression each time the client enters a token indicating a textual break within the command.

15. The method of claim 1, wherein controlling access comprises controlling access to configuration data of a router.

16. A method comprising:

storing configuration data for a device, wherein the configuration data is arranged in the form of a multi-level configuration hierarchy having a plurality of objects, each of the objects having a textual label and representing a portion of the configuration data;

storing authorization data defining an access control attribute and an associated regular expression defining a textual pattern that identifies a set of one or more of the objects within the configuration hierarchy;

applying the regular expression to a command to determine whether the command requests access to any of the objects within the set; and

controlling access to configuration data of the device based on the determination.

17. The method of claim 16, wherein controlling access comprises allowing a client to access to the configuration data represented by the objects requested by the command.

18. The method of claim 16, wherein controlling access comprises denying a client access to the configuration data represented by the objects requested by the command.

19. A method comprising:

receiving input defining an access control attribute and an associated regular expression that specifies a textual pattern;

pre-processing the regular expression to automatically insert one or more meta-characters into the regular expression;

evaluating a command in real-time using the regular expression as a client enters the command via a command line interface; and

controlling access to configuration data of a device based on the evaluation.

20. The method of claim 19, further comprising storing the configuration data in the form of a multi-level configuration hierarchy having a plurality of objects, wherein pre-processing the regular expression comprises automatically inserting one or more meta-characters into the regular expression based on the hierarchical arrangement of the configuration data.

21. The method of claim 19, the regular expression defines a textual pattern that identifies one or more of the objects within the configuration hierarchy, and evaluating the command comprises:

applying the regular expression in real-time to determine whether a portion of the command that has been entered by the client matches the textual pattern; and

selectively allowing the client to complete the command based on the determination.

22. A computer-readable medium comprising instructions for causing a programmable processor to:

store authorization data that defines an access control attribute and an associated regular expression defining a textual pattern;

evaluate a command using the regular expression to determine whether the command matches the textual pattern; and

control access to configuration data of a device based on the evaluation.

23. The computer-readable medium of claim 22, further comprising instructions to cause the programmable processor to allow access to the configuration data when the textual pattern of the regular expression matches the command.

24. The computer-readable medium of claim 22, further comprising instructions to cause the programmable processor to deny access to the configuration data when the textual pattern of the regular expression matches the command.

25. The computer-readable medium of claim 22, further comprising instructions to cause the programmable processor to store authorization data that includes a course-grain access control attribute defining access control rights for respective groups of resources provided by the device, and control access to the configuration data based on the course-grain access control attribute and the evaluation of the regular expression.

26. The computer-readable medium of claim 25, wherein the course-grain access control attribute comprises a set of permission bits, and each of the permission bits is associated with a respective group of the resources.

27. The computer-readable medium of claim 22, further comprising instructions to cause the programmable processor to receive the command from a client via a command line interface.

28. The computer-readable medium of claim 27, further comprising instructions to cause the programmable processor to evaluate the command in real-time while the client inputs the command via the command line interface.

29. The computer-readable medium of claim 22, wherein the configuration data is arranged in the form of a multi-level configuration hierarchy having a plurality of objects, and each of the objects represents a portion of the configuration data that relates to one or more resources of the device.

30. The computer-readable medium of claim 29, wherein the objects have respective textual labels and the regular expression defines the textual pattern to match the textual labels of a set of one or more of the objects within the configuration hierarchy.

31. The computer-readable medium of claim 30, wherein further comprising instructions to cause the programmable processor to apply the regular expression to the command to determine whether the command specifies any of the objects within the set.

32. The computer-readable medium of claim 29, further comprising instructions to cause the programmable processor to pre-process the regular expression to automatically insert one or more meta-characters into the regular expression based on the hierarchical arrangement of the configuration data.

33. The computer-readable medium of claim 29, further comprising instructions to cause the programmable processor to receive the command from a client via a command line interface, and pre-process the regular expression so that the command is evaluated with the regular expression in real-time as the client enters the command.

34. The computer-readable medium of claim 33, further comprising instructions to cause the programmable processor to evaluate the command with the pre-processed regular expression each time the client enters a token indicating a textual break within the command.

35. The computer-readable medium of claim 22, further comprising instructions to cause the programmable processor to control access to configuration data of a router.

36. A device comprising:

a computer-readable medium storing configuration data and authorization data, wherein the authorization data defines an access control attribute and an associated regular expression specifying a textual pattern; and

a management interface that receives a text-based command to access the configuration data, wherein the management interface evaluates the command using the regular expression and controls access to the configuration data based on the evaluation.

37. The device of claim 36, wherein the management interface allows access to the configuration data when the textual pattern of the regular expression matches the command.

38. The device of claim 36, wherein the management interface denies access to the configuration data when the textual pattern of the regular expression matches the command.

39. The device of claim 36, wherein the authorization data includes a course-grain access control attribute defining access control rights for respective groups of resources provided by the device, and the management interface controls access to the configuration data based on the course-grain access control attribute and the evaluation of the regular expression.

40. The device of claim 39, wherein the course-grain access control attribute comprises a set of permission bits, and each of the permission bits is associated with a respective group of the resources.

41. The device of claim 36, wherein the configuration data is arranged in the form of a multi-level configuration hierarchy having a plurality of objects, and each of the objects represents a portion of the configuration data that relates to one or more resources of the device.

42. The device of claim 41, wherein the objects have respective textual labels and the regular expression defines the textual pattern to match the textual labels of a set of one or more of the objects within the configuration hierarchy.

43. The device of claim 42, wherein the management interface applies the regular expression to the command to determine whether the command specifies any of the objects within the set.

44. The device of claim 42, wherein the management interface pre-process the regular expression to automatically insert one or more meta-characters into the regular expression based on the hierarchical arrangement of the configuration data.

45. The device of claim 36, wherein the management interface comprises a command line interface to receive the command from a client, and the management interface evaluates the command with regular expression in real-time as the client enters the command.

46. The device of claim 45, wherein the management interface evaluates the command with the regular expression each time the client enters a token indicating a textual break within the command.

47. The device of claim 36, wherein the device comprises a router.

48. A device comprising:

a computer-readable medium comprising:

configuration data arranged in the form of a multi-level configuration hierarchy having a plurality of objects, each of the objects having a textual label and representing a portion of the configuration data, and

authorization data that defines an access control attribute and an associated regular expression specifying a textual pattern, wherein the textual pattern identifies a set of one or more of the objects within the configuration hierarchy; and

a management interface that applies the regular expression to a command to determine whether the command requests access to any of the objects within the set, and controls access to the configuration data based on the determination.

49. The device of claim 48, wherein based on the determination the management interface allows a client to access to the configuration data represented by the objects requested by the command.

50. The device of claim 48, wherein based on the determination the management interface denies a client access to the configuration data represented by the objects requested by the command.

51. A device comprising:

a computer-readable medium that stores configuration data, and

a management interface that receives input defining an access control attribute and an associated regular expression that specifies a textual pattern, wherein

the management interface pre-processes the regular expression to automatically insert one or more meta-characters into the regular expression, and stores the access control attribute and the pre-processed regular expression as authorization data to control access to the configuration data.

52. The device of claim 51, wherein the management interface further comprises a command line interface to receive a command from a client, wherein the management interface evaluates the command in real-time using the pre-processed regular expression as the client enters the command.

53. A device comprising:

a computer-readable medium storing configuration data and authorization data, wherein the authorization data defines:

a fine-grain access control attribute and an associated regular expression specifying a textual pattern, and

a course-grain access control attribute that defines access control rights for respective groups of resources provided by the device; and

a management interface that evaluates a command received from a client using the regular expression of the fine-grain access control attribute, and controls access to the configuration data based on the course-grain access control attribute and the evaluation of the command.

54. The device of claim 53, wherein the management interface allows access to the configuration data when the course-grain access control attribute does not allow access to a requested portion of the configuration data and the regular expression of the fine-grain access control attribute identifies a match between the command and the textual pattern.

55. The device of claim 53, wherein the management interface denies access to the configuration data when the course-grain access control attribute allows access to a requested portion of the configuration data and the regular expression of the fine-grain access control attribute identifies a match between the command and the textual pattern.